REMARKS

The Office Action dated June 11, 2008 has been received and carefully noted. The above amendments to the claims, and the following remarks, are submitted as a full and complete response thereto.

Claims 1, 8, 9, 12, 15, 16, 19, 20, 24, 27, 31, 33, and 35 have been amended to more particularly point out and distinctly claim the subject matter of the invention. Claims 25, 26 and 28 have been canceled without prejudice or disclaimer. New claims 36-41 have been added. No new matter has been added. Claims 1-24, 27, and 29-41 are currently pending and are respectfully submitted for consideration.

The Office Action rejected claims 1-35 under 35 U.S.C. §103(a) as being unpatentable over 3GPP TS 33.102 v5.1.0 (hereinafter "3G Security") in view of Bacchus (U.S. Patent No. 7,219,223) and UMTS Security (October 2002, Electronics & Communications Engineering Journal, p. 191-204). The Office Action took the position that 3G Security discloses all of the elements of the claims, with the exception of removing the information from the request for registration in the second controller, and the use of a registration request. The Office Action cited Bacchus and UMTS Security as allegedly curing these deficiencies in 3G Security.

Claim 1, upon which claims 2-14 are dependent, recites a method including receiving a request for registration from a user equipment at a serving controller via a second controller. The request for registration including information indicative of at least one protocol supported by the user equipment. The method further includes determining,

based on the information, in the second controller that the user equipment supports a second protocol other than a first protocol. The method also includes removing the information from the request for registration in the second controller, including in the request for registration an indication that the second protocol is used by the user equipment and forwarding the request for registration including said indication to the serving controller, and sending a challenge in accordance with the second protocol from the serving controller to the user equipment via the second controller.

Claim 15, upon which claims 16-23 are dependent, recites a system including a serving controller configured to accept registrations of user equipments and to support at least two different protocols. The system further includes a second controller configured to receive from a user equipment in a request for registration data indicative of at least one protocol that the user equipment supports, to remove said data from the request for registration, to provide the serving controller with information regarding a protocol supported by the user equipment that has requested to be registered to the serving controller, and to forward the request for registration to the serving controller. The serving controller is configured to send a challenge in accordance with a determined protocol to the user equipment and to authenticate a message from the user equipment based on a response to the challenge included in the message.

Claim 24, upon which claims 29-34 are dependent, recites an apparatus including a receiver configured to receive a request for registration from a user equipment for forwarding to a serving controller. The request includes data indicative of at least one

protocol supported by said user equipment. The apparatus further includes a controller configured to determine based on said data a protocol supported by the user equipment that has requested to be registered to the serving controller, to remove the data from the request for registration in the second controller before forwarding said request to the serving controller, and to signal information to the serving controller regarding the protocol supported by the user equipment.

Claim 27 recites an apparatus including receiving means for receiving a request for registration from a user equipment for forwarding to a serving controller, said request including data indicative of at least one protocol supported by said user equipment. The apparatus further includes determining means for determining, based on said data, a protocol supported by the user equipment that has requested to be registered to the serving controller, removing means for removing the data from the request for registration in the second controller before forwarding said request to the serving controller, and signaling means for signaling information to the serving controller regarding the protocol supported by the user equipment.

Claim 35 recites a computer program embodied on a computer readable medium, the computer program is configured to control a processor to perform a method. The method includes receiving a request for registration from a user equipment at a serving controller via a second controller. The request for registration includes information indicative of at least one protocol supported by the user equipment. The method further includes determining, based on the information, in the second controller that the user

equipment supports a second protocol other than a first protocol, removing the information from the request for registration in the second controller, including in the request for registration an indication that the second protocol is used by the user equipment and forwarding the request for registration including said indication to the serving controller, and sending a challenge in accordance with the second protocol from the serving controller to the user equipment via the second controller.

Claim 36, upon which claims 37-40 are dependent, recites a method including receiving a request for registration from a user equipment for forwarding to a serving controller. The request includes data indicative of at least one protocol supported by the user equipment. The method further includes determining, based on said data, a protocol supported by the user equipment that has requested to be registered to the serving controller, removing the data from the request for registration in the second controller before forwarding said request to the serving controller, and signaling information to the serving controller regarding the protocol supported by the user equipment.

Claim 41 recites a computer program embodied on a computer readable medium, the computer program is configured to control a processor to perform a method. The method includes receiving a request for registration from a user equipment for forwarding to a serving controller. The request includes data indicative of at least one protocol supported by said user equipment. The method further includes determining, based on said data, a protocol supported by the user equipment that has requested to be registered to the serving controller, removing the data from the request for registration in the second

controller before forwarding said request to the serving controller, and signaling information to the serving controller regarding the protocol supported by the user equipment.

As will be discussed below, the cited prior art fails to disclose or suggest all of the elements of the claims, and therefore fails to provide the advantages and features discussed above.

3G Security generally describes 3G security procedures performed within 3G networks. Five security feature groups are defined, including network access security, network domain security, user domain security, application domain security, visibility and configurability of security.

Bacchus generally describes a client that transmits its cipher suite list to the load balancer. A cipher suite match is then determined based on that list and a mapping of cipher suite names to services (column 9 lines 24 to 33). A new SSL connection is then established using the encryption capabilities associated with the cipher suite match to allow the client to receive data in encrypted form.

UMTS Security discloses an IMS subsystem using SIP. Fig. 7 of UMTS Security shows illustratively message flow for a registration request from a user equipment to a S-CSCF.

The combination of 3G Security, Bacchus and UMTS Security fails to disclose or suggest all of the elements of the present claims. For example, 3G Security, Bacchus and UMTS Security, whether considered individually or combined, do not disclose or suggest

"determining, based on the information, in the second controller that the user equipment supports a second protocol other than a first protocol," as recited in claim 1 and similarly recited in claim 35. The combination of 3G Security, Bacchus, and UMTS Security also fails to disclose or suggest "a second controller configured to receive from a user equipment in a request for registration data indicative of at least one protocol that the user equipment supports, to remove said data from the request for registration, to provide the serving controller with information regarding a protocol supported by the user equipment that has requested to be registered to the serving controller," as recited in claim 15. Similarly, 3G Security, Bacchus, and UMTS Security fail to disclose or suggest "determining, based on said data, a protocol supported by the user equipment that has requested to be registered to the serving controller," as recited in claim 36 and similarly recited in claims 24, 27, and 41.

3G Security discloses, in figure 14, a mechanism at connection establishment for authentication and for determining appropriate UMTS integrity and encryption algorithms (UIAs and UEAs). An MS transfer, included in UE, of security capability information UIAs and UEAs supported by the MS is made to an SRNC (step 1). The MS is authenticated at step 3. At step 6, the SRNC decides which algorithms to use based on UIAs and UEAs allowed by an SGSN/VLR and the UIAs and UEAs in the UE security information. Generally, steps 5 to 11 relate to establishment of a security mode. In the security mode, both the SRNC and the MS have respective ciphering/deciphering algorithms allowing secure communication.

The claimed invention differs conceptually from the disclosure of 3G Security because the claimed invention does not concern negotiation of algorithms. Rather, embodiments of the present invention are directed, in part, to determining that the user equipment supports a second security mechanism comprising a *second protocol* other than a first security mechanism comprising a *first protocol*. 3G Security does not disclose or suggest making such a determination and, therefore, fails to disclose the limitations of the independent claims outlined above.

Bacchus and UMTS Security also fail to disclose or suggest, at least, determining that the user equipment supports a second security mechanism comprising a *second protocol* other than a first security mechanism comprising a *first protocol*. Accordingly, Bacchus and UMTS Security fail to cure the deficiencies in 3G Security.

Furthermore, none of the cited references teach or address the problems that the claimed invention overcomes. In particular, a problem addressed by the claimed invention is that if a request for registration does not include a list containing an indication that a default security mechanism, such as 3GPP IPSec, is supported, registration with a serving controller will not be allowed to proceed. The claimed invention advantageously enables a user equipment not supporting such a default security mechanism to register to the serving controller (Specification, page 20, lines 1-5) in such a way as to allow secure communication, for example including integrity protection, with the user equipment. The combination of 3G Security, Bacchus and UMTS Security do

not disclose or suggest all of the elements of the present claims and, therefore, do not serve to overcome these problems.

In view of the above, Applicants respectfully submit that 3G Security, Bacchus and UMTS Security, whether considered individually or combined, do not disclose or suggest "determining, based on the information, in the second controller that the user equipment supports a second protocol other than a first protocol," as recited in claim 1 and similarly recited in claim 35. The combination of 3G Security, Bacchus, and UMTS Security also fails to disclose or suggest "a second controller configured to receive from a user equipment in a request for registration data indicative of at least one protocol that the user equipment supports, to remove said data from the request for registration, to provide the serving controller with information regarding a protocol supported by the user equipment that has requested to be registered to the serving controller," as recited in claim 15. Similarly, 3G Security, Bacchus, and UMTS Security fail to disclose or suggest "determining, based on said data, a protocol supported by the user equipment that has requested to be registered to the serving controller," as recited in claim 36 and similarly recited in claims 24, 27, and 41. Therefore, Applicants respectfully request that the rejections of claims 1, 15, 24, 27, 35, 36, and 41 be withdrawn.

Claims 2-14, 16-23, 29-34, and 37-40 are dependent upon claims 1, 15, 24, and 36, respectively. As such, claims 2-14, 16-23, 29-34, and 37-40 should be allowed for at least their dependence upon claims 1, 15, 24, and 36, and for the specific limitations recited therein.

For at least the reasons discussed above, Applicants respectfully submit that the cited prior art fails to disclose or suggest all of the elements of the claimed invention. These distinctions are more than sufficient to render the claimed invention unanticipated and unobvious. It is therefore respectfully requested that all of claims 1-24, 27, and 29-41 be allowed, and this application passed to issue.

If for any reason the Examiner determines that the application is not now in condition for allowance, it is respectfully requested that the Examiner contact, by telephone, the applicants' undersigned representative at the indicated telephone number to arrange for an interview to expedite the disposition of this application.

In the event this paper is not being timely filed, the applicants respectfully petition for an appropriate extension of time. Any fees for such an extension together with any additional fees may be charged to Counsel's Deposit Account 50-2222.

Respectfully submitted,

Majid S. AlBassam
Registration No. 54,749

Customer No. 32294
SQUIRE, SANDERS & DEMPSEY LLP
14TH Floor
8000 Towers Crescent Drive
Vienna, Virginia 22182-6212
Telephone: 703-720-7800
Fax: 703-720-7802

Enclosures: Petition for Extension of Time
Additional Claim Fee transmittal